UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/641,868	08/18/2000	Erwin Hess	GR 98 P 1180 P	7548

24131 7590 11/22/2004

LERNER AND GREENBERG, PA
P O BOX 2480
HOLLYWOOD, FL 33022-2480

EXAMINER	
TESLOVICH, TAMARA	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 11/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/641,868	HESS ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 August 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

The drawings are objected to because they do not include suitable descriptive legends as per 37 CFR 1.84(o). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Claim 9 is objected to because of the following informalities: page 28, line 11 is incomprehensible due to either a missing word or incorrect word order. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Myaji et al ("Efficient Elliptic Curve Cryptosystems") and further in view of Menezes ("Elliptic Curve Cryptosystems").

As per claim 1, Menezes discloses a method of cryptographic processing on a computer, which comprises the steps of: Prescribing an elliptic curve in a first form, the elliptic curve having a plurality of first parameters; transferring the elliptic curve into a second form $y^2 = x^3 + c^2ax + c^3b$ by determining a plurality of second parameters, wherein at least one of the second parameters is shortened in length by comparison with the first parameter; wherein x, y are variables; a, b are the first parameters; and c is a constant; wherein at least the parameter a is shortened by selecting the constant c such that $c^4a \bmod p$ is determined to be

significantly shorter than a length of the parameter b and the length of the prescribed variable p; and determining the elliptic curve in the second form for cryptographic processing (see preface and pages 13, 99-100).

Menezes fails to disclose the use of a second equation of the form $y^2 = x^3 + c^4ax + c^6b$.

Miyaji et al further explores the area of efficient elliptic curve exponentiation for use in elliptic curve cryptosystems, specifically mentioning the use of a second equation of the form $y^2 = x^3 + c^4ax + c^6b$ (see page 3).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Menezes' elliptic curve cryptosystem Miyaji et al's second equation of form $y^2 = x^3 + c^4ax + c^6b$ to improve performance and reduce key size.

As per claim 2, the modified Menezes and Miyaji et al system discloses the method according to claim 1, wherein the first form of the elliptic curve is defined by $y^2 = x^3 + ax + b$ (see Miyaji et al page 3 and Menezes page 100).

As per claim 3, the modified Menezes and Miyaji et al system discloses the method according to claim 1, which comprises carrying out cryptographic encoding (see Menezes pages 4, 13, 97).

As per claim 4, the modified Menezes and Miyaji et al system discloses the method according to claim 1, which comprises carrying out cryptographic decoding (see Menezes pages 4, 13, 97).

As per claim 5, the modified Menezes and Miyaji et al system discloses the method according to claim 1, which comprises carrying out key allocation (see Menezes pages 4-5).

As per claim 6, the modified Menezes and Miyaji et al system discloses the method according to claim 1, which comprises carrying out a digital signature (see Menezes pages 4-5, 10-12, 97).

As per claim 7, the modified Menezes and Miyaji et al system discloses the method according to claim 6, which comprises carrying out a verification of the digital signature (see Menezes pages 4-5, 10-12, 97).

As per claim 8, the modified Menezes and Miyaji et al system discloses the method according to claim 1, which comprises carrying out an asymmetrical authentication (see Menezes pages 4-5).

As per claim 9, Menezes discloses a processor unit, within a device for cryptographic processing, programmed to: prescribe an elliptic curve in a first form, with a plurality of first parameters determining the elliptic curve; transform the elliptic curve into a second form $y^2 = x^3 + c^2ax + c^3b$ by determining a plurality of second parameters, at least one of the second parameters being shortened in length by comparison with the first parameter; wherein x, y are variables; a, b are the first parameters; and c is a constant; shorten the at least the parameter a by selecting the constant c such that $c^4a \bmod p$ can be determined to be much shorter than the length of the parameter b and the length of the prescribed variable p; and determine the elliptic curve in the second form for the purpose of cryptographic processing (see preface and pages 13-14, 99-100).

Menezes fails to disclose the use of a second equation of the form $y^2 = x^3 + c^4ax + c^6b$.

Miyaji et al further explores the area of efficient elliptic curve exponentiation for use in elliptic curve cryptosystems, specifically mentioning the use of a second equation of the form $y^2 = x^3 + c^4ax + c^6b$ (see page 3).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Menezes' elliptic curve cryptosystem Miyaji et al's second equation of form $y^2 = x^3 + c^4ax + c^6b$ to improve performance and reduce key size.

As per claim 10, the modified Menezes and Miyaji et al system discloses the device according to claim 9, wherein the device is embodied as a chip card with memory area, the memory area being adapted to store the parameters of the elliptic curve (see Menezes pref and pages 13-14, 99).

As per claim 11, the modified Menezes and Miyaji et al system discloses the device according to claim 10, wherein the chip card has a protected memory area adapted to store a secret key (see Menezes pref and pages 13-14, 99).

As per claim 12, Menezes discloses a computer-readable medium having computer-executable instructions for performing a cryptographic processing method which comprises the steps of: prescribing an elliptic curve in a first form, the elliptic curve having a plurality of first parameters; transforming the elliptic curve into a second form $y^2 = x^3 + c^2ax + c^3b$ by determining a plurality of second parameters, wherein at least one of the second parameters is shortened in length by comparison with the first parameter; wherein x, y are variables; a, b are the

first parameters; and c is a constant; wherein at least the parameter a is shortened by selecting the constant c such that c^4a mod p is determined to be significantly shorter than the length of the parameter b and the length of the prescribed variable p; and determining the elliptic curve in the second form for cryptographic processing (see pref and pages 13-14, 99-100).

Menezes fails to disclose the use of a second equation of the form $y^2 = x^3 + c^4ax + c^6b$.

Miyaji et al further explores the area of efficient elliptic curve exponentiation for use in elliptic curve cryptosystems, specifically mentioning the use of a second equation of the form $y^2 = x^3 + c^4ax + c^6b$ (see page 3).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Menezes' elliptic curve cryptosystem Miyaji et al's second equation of form $y^2 = x^3 + c^4ax + c^6b$ to improve performance and reduce key size.

As per claim 13, the modified Menezes and Miyaji et al system discloses the computer-readable medium according to claim 12, wherein the first form of the elliptic curve is defined by $y^2 = x^3 + ax + b$ (see Miyaji et al page 3 and Menezes page 100).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell
Andrew Caldwell